ISSN 0956-9979 APRIL 1997

VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL

Editor: **Ian Whalley**

Assistant Editor: **Megan Skinner**

Technical Editor: **Jakub Kaminski**

Consulting Editors:

Richard Ford, IBM, USA
Edward Wilding, Network Security, UK

IN THIS ISSUE:

• **In Indian interests.** Continuing our occasional series on the state of the virus field in various parts of the world, this month sees *VB* in India. To learn more about the situation there, turn to p.16.

• **Sharing the load.** ShareFun is a WordBasic virus which exhibits an interesting new technique. Turn to p.10 to learn more.

• **Administration problems.** A new turn for the comparative review; this month we look at the remote and centralized administration offered by network anti-virus packages. Who has what? See p.11.

CONTENTS

VIRUS BULLETIN **©1997 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. /97/$0.00+2.50** No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

EDITORIAL

Goodbye, Cruel World

Over the last few hours I've been looking back at past editions of *VB* – two in particular. Twice before the farewell editorial has come around, and imagine my annoyance when I discovered that the obvious pun was used on the first of these. Yes, I had wanted to have a 'Terminate and Stay Resident' title for my swan-song, but it was not to be: Ed Wilding beat me to it by more than three years. Yes, the time has come for me to move on; in some ways it seems that I've been doing this job for years and years, in others it only seems a few months since I moved into the editor's chair. In reality, two years have passed since that day; two years I have enjoyed to the full.

> *“ the rise in the macro virus is … perhaps the most significant development … since the first PC virus ”*

In those years, a lot has happened – I have been threatened with everything from withdrawal of subscriptions to the attentions of large numbers of (no doubt vastly overpaid) lawyers; I have been arrested, deafened by alarms, and spent more time on aeroplanes than I care to remember (and I'm still scared of flying!). Fortunately, the subscriptions were not withdrawn, the lawyers were put firmly back in their offices, the arrests were only as part of a police role-playing exercise, the alarms turned out to be false, and the 'planes? Well, not a lot can be done about them.

In all seriousness, the part of the job I have both most enjoyed and most hated was dealing with the people who work in the anti-virus field. It is a world full of remarkable levels of cooperation, countered (in many cases within the same companies!) by remarkable levels of bitterness and competition. Underneath the surface, the people who do the work are determined and helpful – it is merely unfortunate that they often have to work for less scrupulous individuals.

At the same time, nothing changes. The same industry players are, to a greater or lesser extent, still around. There have been mergers and sell-offs, but the industry has been reasonably static over the last two years, certainly when compared with the previous two. Many scanners appear not to have changed at all, other than to cope with the meteoric rise in the number of viruses detected.

As far as viruses go, *plus ça change, plus c'est la même chose*. Macro viruses changed everything. Compare, for example, this month's prevalence table with that of two years ago; the rise in the macro virus is clear; and is probably the most significant development in the field since the first PC virus.

What's next? Who can say – predictions are a tricky thing. However, it seems the period of consolidation is set to continue, with vendors branching further from the anti-virus field. To some extent, we see this already: backup and anti-virus utilities, for example, are becoming ever more intertwined.

When I first became involved with viruses, I thought they would die out as DOS' star waned; that as more modern OSs took over, the computer virus researchers would be out of a job. In many ways, I wish I still believed this. In my opinion, it is time that will make the difference: as computers become more and more part of society, the ethics of using them will become more clearly defined. There will always be some who flout the accepted ethical norms, but it is to be hoped that the problem will decline as familiarity with computers grows.

In terms of computer security, there are boom times ahead. As the Internet continues its path towards world domination, organisations leave themselves increasingly open to risk; lured by its charms, more and more are sure to fall foul of its multitudinous dangers. These dangers include viruses, but not as the media expect, in the form of 'rogue Java applets'. As we are pulled towards the supposed ideal of 'the Internet as part of the desktop', as the boundary between 'ours' and 'theirs' is blurred still further, few people stop to think, 'But what if I don't trust what's theirs?' These days, the concept of wishing to remain an island, apart from the teeming electronic world, seems strange…

To return to the immediate matter in hand, I vacate the chair of power to return to the world of programming. For a computer weenie such as myself, it is the best place to be. I leave it to my successor to introduce himself on his arrival. My presence in *Virus Bulletin* will remain, in the form of contributions to the magazine, but as far as editorials are concerned, this is my farewell.

NEWS

Patrolling UseNet

For several years, the problem of viruses spreading by being posted to UseNet newsgroups has been a very real one – the postings of viruses such as Kaos4, Hare, and (more recently) Tentacle to certain newsgroups are well known. A new approach to the problem has just been launched by the UK-based *Dr Solomon's Software* (formerly known as *S&S International*); called *VirusPatrol*, the system scans messages posted to newsgroups for the presence of viruses.

The nature of UseNet is such that this is a reactive solution. It is not possible to stop infected messages being sent (although it would be possible to send so-called 'cancel messages' to prevent offending items from propagating, this would be unwise from a netiquette point of view): *VirusPatrol* can only warn about the presence of a virus in a previously-posted message. However, this has benefits as far as the Internet-user is concerned: he is able to tell that he is at risk if he unpacked the relevant attachment, or even from a particular individual.

VirusPatrol does not form a 'product' per se – it is not available for purchase. Instead, its results are made available as a free service by *Dr Solomon's*, both as postings to the newsgroups concerned and (in the near future) as a listing on their WWW site (http://www.drsolomon.com/).

It remains to be seen whether or not postings by the system (which has been in testing since the beginning of 1997, and has generated quite a number of warnings) work simply as a warning that a virus was posted, a deterrent to the user posting viruses, or an encouragement to others – it is possible that people may post viruses in an attempt to trigger the system… ■

VB'97 Update

Readers are reminded that the seventh annual *Virus Bulletin Conference* will take place in San Francisco, California, on 2/3 October 1997. The progamme is already in place, and the conference brochure will shortly be sent to subscribers, and to delegates of previous conferences. Advance registration is now being accepted; email alie@virusbtn.com, or Tel +44 1235 555139, for details ■

Correction

In last month's *NetWare* comparative review (see *VB*, March 1997, p.11), a result was published in error: *Command Software's F-PROT Professional's* score against the polymorphic test-set was listed as detecting 11,000 samples and scoring 100%; it actually detected 6064 samples, scoring 49.3%. We apologise for the error, which will be corrected in reprints or electronic versions of the article, and thank *Frisk Software International* for pointing out the mistake ■

Prevalence Table – February 1997

Virus	Type	Incidents	Reports
Concept	Macro	72	15.3%
NPad	Macro	61	13.0%
Form	Boot	30	6.4%
MDMA	Macro	28	6.0%
AntiEXE.A	Boot	25	5.3%
Wazzu	Macro	22	4.7%
Parity_Boot.B	Boot	20	4.3%
AntiCMOS	Boot	19	4.0%
Empire.Monkey.B	Boot	15	3.2%
Junkie	Multi	15	3.2%
Ripper	Boot	14	3.0%
NYB	Boot	9	1.9%
WelcomB	Boot	9	1.9%
Johnny	Macro	8	1.7%
Stoned.Angelina	Boot	8	1.7%
Bandung	Macro	6	1.3%
Edwin	Boot	5	1.1%
Hassle	Macro	5	1.1%
Helper	Macro	5	1.1%
Jumper.B	Boot	5	1.1%
Quandary	Boot	5	1.1%
Stealth_Boot.C	Boot	5	1.1%
Imposter	Macro	4	0.9%
Laroux	Macro	4	0.9%
Sampo	Boot	4	0.9%
ShowOff	Macro	4	0.9%
Empire.Monkey.A	Boot	3	0.6%
One_Half.3544	Multi	3	0.6%
Stoned.NoInt	Boot	3	0.6%
Other[1]		54	11.5%
Total		470	100%

[1] The Prevalence Table includes two reports of each of the following viruses: Colors.C, Die_Hard, EXEBug, Lunch, Manzon, Natas.4744, ShareFun, Swiss_Boot, Taipan.438, Tentacle, and Tequila.

It also includes one report of each of the following viruses: Arya.4616, Barrotes.1310, Boot.437, CA, Colors.B, Comp.2052, Divina, FatAvenger, Hare.7601, Havoc.3072, Hybrid, Int40, Irish, J&M, Moloch, Niceday, Nuclear, Pasta, Rapi, Rapi.C, Rhubarb, Satria, SheHas, Shell.10634, Stat, Stoned.NOP, Stoned.Spirit, Stoned.Stonehenge, Telefonica, TPVO.3783, Tubo, and V-Sign.

IBM PC VIRUSES (UPDATE)

The following is a list of updates and amendments to the *Virus Bulletin Table of Known IBM PC Viruses* as of 21 March 1997. Each entry consists of the virus name, its aliases (if any) and the virus type. This is followed by a short description (if available) and a 24-byte hexadecimal search pattern to detect the presence of the virus with a disk utility or a dedicated scanner which contains a user-updatable pattern library.

Type Codes

C	Infects COM files	**M**	Infects Master Boot Sector (Track 0, Head 0, Sector 1)
D	Infects DOS Boot Sector (logical sector 0 on disk)	**N**	Not memory-resident
E	Infects EXE files	**P**	Companion virus
L	Link virus	**R**	Memory-resident after infection

Ahav.337

CN: An appending, 337-byte virus containing the texts '[AHaV]' and 'DHA 9/2/95'.

```
Ahav.337          8986 3B02 B440 B951 018D 9600 01CD 21B8 0042 33C9 33D2 CD21
```

Ahav.379

CN: An encrypted, appending, 379-byte virus containing the texts '[AHaV]', 'Gothmog/DHA' and '*.COM'.

```
Ahav.379          8986 2702 B440 B97B 018D 9600 01CD 21B8 0042 33C9 33D2 CD21
```

Ahav.385

CN: An encrypted, appending, 385-byte virus containing the texts '[AHaV]', 'Gothmog/DHA' and '*.COM'.

```
Ahav.385          8986 2D02 B440 B981 018D 9600 01CD 21B8 0042 33C9 33D2 CD21
```

Arianna.3076

CER: A stealth, encrypted, appending, 3076-byte virus containing the texts 'Improved ARIANNA , waiting for ADVANCED 386Bari @1995 by AV(ANTI)-VIRUS SYSTEM', '.exe', '.com', '.EXE' and '.COM'. All infected files have their time-stamp set to 62 seconds.

```
Arianna.3076      8BFE 03FC 368A 45D4 2846 0080 ??00 ??49 7806 4D4E 79EA EBE5
```

AuntB.727

CEN: An appending, 727-byte virus containing the texts '[BW]', 'AuntB (c) by HypoDermic!! Part of the Mayberry Family!!!' and '*.*'. The virus infects three files at a time.

```
AuntB.727         96DA 03CD 21B4 40B9 D402 8D96 0601 CD21 32C0 E828 008D 96D6
```

BladeRunner

CER: A family of stealth, encrypted viruses which marks infected files with a time-stamp set to 2 seconds. 831 contains the text 'Blade Runner Virus'. The 845-byte variant contains the message 'Blade Runner Virus, Time to Die!'. Variant 860 contains the text 'Blade Runner Virus, were men there, police men!'.

```
BladeRunner.831   01FA B845 5992 CD10 9292 9292 9292 92BB ???? BF9F 012E 8107
BladeRunner.845   01FA B845 5992 CD10 9292 9292 9292 92BB ???? BFA6 012E 8107
BladeRunner.860   01FA B845 5992 CD10 9292 9292 9292 92BB ???? BFAD 012E 8107
```

BW.735

CEN: An appending, 735-byte virus containing the texts 'RESISTANCE IS FUTILE THIS PROGRAM IS INFECTED WITH 2FIRST CONTACT!' and '*.*'. Infected EXE files have the value SP set to 4F4Fh ('OO').

```
BW.735            B440 B9DC 0290 8D96 0601 CD21 32C0 E828 008D 96DE 03CD 215A
```

Danish_Tiny.308

CN: An encrypted, appending, 308-byte virus containing the texts '*.COM', 'Tiny-F version 1.1' and 'Released 10-19-91'. The virus infects only files starting with an initial near jump (E9h).

```
Danish_Tiny.308   B9DA 00D1 E973 014E 8BFE AD33 C3AB E2FA 5E59 5B58 C3E8 DCFF
```

Dust.1088

CER: A stealth, encrypted, appending, 1088-byte virus containing the texts 'Dead to Windows!' and 'Dracula lives Resucitated somewhere in time by Dust Group, Tucumán, Argentina'.

```
Dust.1088         B902 022E 8B3C F7D7 23FA F7D2 2E21 142E 093C F7D2 4646 E2EB
```

Emhaka.749

CER: An appending, 749-byte virus containing the text '(c)10-1994 Emhaka!'.

```
Emhaka.749        83EE 03B8 FFFF CD21 3D00 0074 040E E837 002E 81BC A202 4D5A
```

Gomer.691

CEN: An appending, 691-byte virus containing the texts '[BW]', 'GoMer (G.O.L) by HypoDermic!! Part of the Mayberry Family!!!' and '*.*'.

```
Gomer.691         B603 CD21 B440 B9B0 0290 8D96 0601 CD21 32C0 E828 008D 96B2
```

HLLO.6224

EN: An overwriting, 6224-byte virus containing the texts 'c:\dos\msc.dat', 'dosshell.hlp', 'dosshell.exe', 'C:\docas\*.*', '*.exe', and a long list of messages: 'runme', 'test', 'info', 'hw-test', 'cache_t', 'memory', 'part-infstart', 'begin', 'show', 'Hardware compatibility O.K.' 'No errors in memory Bank 0', 'IBM PC compatibility 97 %', 'Interleave factor 1:2', 'cache hit rate: 81 %', '70 ns RAM memory', 'Partition sector is O.K.', 'You can start main program', 'Now begin work on your application', 'sVGA compatibility 96%'.

```
HLLO.6224         2687 4D08 268B 1DB4 40CD 2172 072B C174 03B8 6500 1FCA 0400
```

Immortal.377

CN: An encrypted, appending, 377-byte direct infector containing the texts 'iMMoRTaL.377 {Encrypted!!}' and '.com'.

```
Immortal.377      8896 4001 E80F 00B4 40B9 7901 8D96 0001 CD21 E801 00C3 B933
```

Immortal.510

CN: An encrypted, appending, 510-byte direct infector (two minor variants, A and B) containing the texts 'iMMoRTaL.510 {Encrypted!!}' and '*.com'.

```
Immortal.510      CA01 E80F 00B4 40B9 FE01 8D96 0001 CD21 E801 00C3 B92E 018D
```

Immortal.550

CN: An appending, 550-byte direct infector containing the encrypted texts ‘iMMoRTaL.550!!’, ‘.com’, ‘anti-vir.dat’, ‘c:\dos\keyb.com’, ‘c:\dos\doskey.com’ and ‘c:\run-me.com’. The virus disables TBSCANX and drops the file ‘RUN-ME.COM’.

```
Immortal.550        8986 1F03 B440 B926 028D 9600 01CD 21B8 0042 2BC9 99CD 21B4
```

Insert.258

CR: An encrypted, prepending, 258-byte virus containing the text ‘[Insert v 1.7] [Darkman/VLAD]’. The following template detects the virus in memory only.

```
Insert.258          BF06 01E8 F200 B802 63CD 213B C374 368C D848 8ED8 33FF 803D
```

Jeru.CVEX4.5120.B

CER: Based on Jeru.CVEX4.5120, prepending (COM) and appending (EXE), this 5120-byte variant contains the texts ‘COMMAND.COM’, ‘IBMBIO.COM’, ‘IBMDOS.COM’, ‘PV’, ‘AI’, ‘TRACER’, ‘VB’, ‘TRMATE’, ‘TPLUS’, ‘ZTEST’, ‘ZLOCK’, ‘CHKLIST.MS’, ‘CHKLIST.CPS’, ‘PVTSR.COD’, ‘DR.MIT’, ‘PVSCAN.COD’, ‘PVCLEAN.COD’, ‘ZTEST.BIN’, ‘AISCLN.COD’, and ‘GSCAN.DAT’. On 10 July it displays the message ‘This is Corsair Virus v1.0 Written by Dark Rascal in Taichung, Taiwan, <R.O.C>.’.

```
Jeru.CVEX4.5120.B   FCB8 60AC CD21 3DFF AC75 1233 C0B8 60EC 2E8B 0E07 01BF 0001
```

Kode

CN: A family of appending, direct infectors containing the text ‘*.COM’. Variants 328 and 329 contain the additional message ‘GRAPHIC CARD UNABLE TO PILOT YOUR FUCKED MONITOR’. Variants 335 and 336 contain the text ‘????????.COM’ and ‘GRAPHIC CARD UNABLE TO PILOT YOUR STUPID MONITOR’.

```
Kode.145            B440 8D94 0301 B991 00CD 21B4 3ECD 21B4 4FCD 2172 02EB 9BC3
Kode.147            B440 8D94 0301 B993 00CD 21B4 3ECD 21B4 4FCD 2172 02EB 9AC3
Kode.172            B440 BA03 0103 D6B9 AC00 CD21 B43E CD21 B44F CD21 7202 EB96
Kode.174            B440 BA03 0103 D6B9 AE00 CD21 B43E CD21 B44F CD21 7202 EB95
Kode.216            BA03 0103 D6B9 D800 B440 CD21 5A59 B457 B001 CD21 B43E CD21
Kode.217            BA03 0103 D6B9 D900 B440 CD21 5A59 B457 B001 CD21 B43E CD21
Kode.328            BA03 0103 D6B9 4801 B440 CD21 5A59 B457 B001 CD21 B43E CD21
Kode.329            BA03 0103 D6B9 4901 B440 CD21 5A59 B457 B001 CD21 B43E CD21
Kode.335            BA03 0103 D6B9 4F01 B440 CD21 5A59 B457 B001 CD21 B43E CD21
Kode.336            BA03 0103 D6B9 5001 B440 CD21 5A59 B457 B001 CD21 B43E CD21
```

Monster.531

CN: An appending, 531-byte, direct infector containing the texts ‘[MONSTER]\’, ‘*.*’ and ‘*.COM’. All infected files have the word 3412h located at the end of code.

```
Monster.531         B440 B913 028B D6CD 215A 59B8 0157 CD21 59E8 4700 E85B 00B4
```

Monster.55?

CN: A group of three encrypted, appending, direct infectors containing the texts ‘\’, ‘*.*’ and ‘*.COM’. All infected files have the word 3412h located at the end of code.

```
Monster.554         BE?? ??80 74FA ??80 74FD ??EB 00B0 ??B9 1002 ??30 04?? E2FB
Monster.555         BE?? ??80 74FA ??80 74FD ??EB 00B0 ??B9 1102 ??30 04?? E2FB
Monster.557         BE?? ??80 74FA ??80 74FD ??EB 00B0 ??B9 1302 ??30 04?? E2FB
```

Monster.6??

CN: A group of six encrypted, appending, direct infectors containing the texts ‘[MONSTER]\’, ‘*.*’ and ‘*.COM’. All infected files have the word 3412h located at the end of code.

```
Monster.633         BE?? ??80 74FA ??80 74FD ??EB 00B0 ??B9 5f02 ??30 04?? E2FB
Monster.640         BE?? ??80 74FA ??80 74FD ??EB 00B0 ??B9 6602 ??30 04?? E2FB
Monster.641         BE?? ??80 74FA ??80 74FD ??EB 00B0 ??B9 6702 ??30 04?? E2FB
Monster.657         BE?? ??80 74FA ??80 74FD ??EB 00B0 ??B9 7702 ??30 04?? E2FB
Monster.661         BE?? ??80 74FA ??80 74FD ??EB 00B0 ??B9 7B02 ??30 04?? E2FB
Monster.662         BE?? ??80 74FA ??80 74FD ??EB 00B0 ??B9 7C02 ??30 04?? E2FB
```

Nomercy.575

CER: An appending, 575-byte virus dropped by the macro virus ShowOff.G. The virus contains the plain-text message ‘This is a drop virus form NoMercy 0.1b [Macro Virus]’.

```
Nomercy.575         1E06 E800 005D 81ED 0B00 B878 B8CD 2181 FA1A CB74 328C C048
```

Ramesy.336

CN: A prepending, 336-byte virus containing the texts ‘[RAMESY]’, ‘Coaxial Karma/94’, ‘*.COM’ and ‘????????COM’. The virus corrupts short files and reinfects already infected ones.

```
Ramesy.336          E844 0157 BE00 01B9 A800 A5E2 FD5D 8D96 1400 FFE2 BF00 0157
```

Simbioz.331

CN: An appending, 331-byte virus containing the texts ‘*.com’ and ‘[Simbioz.Inside]’. It takes control by patching the instruction sequence inside the file. It looks for the code ‘MOV AH, ??; INT 21h (BA?? CD21)’ and replaces it with a call to the attached virus code. The original variable byte is stored at the end of the infected file. Simbioz reinfects already infected files.

```
Simbioz.331         B440 B94B 0190 0E1F 8BD5 CD21 720C 2EA1 F400 241F 0407 2EA3
```

Tigre.1795

CER: A stealth, encrypted, appending, 1795-byte virus containing the texts ‘C:CHKLIST.MS’, ‘C:CHKLIST.CPS’, ‘C:ZZ##.IM’, ‘anti-vir.dat’, ‘ANTI-VIR.DAT’, ‘DIGITAL ANARCHY’ and ‘Virus TIGRE v1.0 - (c) 1995 Escrito por El Cancerbero [DAN] 17/02/95 - Argentina’.

```
Tigre.1795          8DB6 4F00 8BFE B9B4 06B4 02CD 173E 8A96 3700 3E8A B638 00EB
```

Trivial.50

CER: An overwriting, memory-resident, 50-byte virus which replaces every file loaded for execution with its own code.

```
Trivial.50          B801 3C33 C9CD 2193 0E1F B440 99FE C6B1 32CD 21CF 80FC 4B74
```

V.357

CR: A stealth, prepending, 357-byte virus marking all infected files with a time-stamp set to 62 seconds.

```
V.357               B440 33D2 B965 0151 E81F 00B8 0042 33C9 33D2 E815 00B4 400E
```

INSIGHT

Carey on Symantec

Carey Nachenberg is not a name well-known outside anti-virus circles; inside, however, it is a different story. A programmer who is fast becoming a top-class researcher, *Symantec* would be wise to retain his services.

Learning to Fly

At eleven, Nachenberg was given a 16K TI 99-4A by his father, and told that if he wanted to play games, he'd have to program them himself. He was a teenager when he obtained his first PC; a 256K *IBM*: 'It had nice graphics, and Basic. I ended up running a programming Bulletin Board. We'd exchange source code, and talk about programming – it taught me a lot.'

By the time he reached high school, Nachenberg was an advanced programmer: he sat the university entrance exam for computer studies in his first year there, 'to get it out of the way'. This left his high school years free to learn C and other programming languages, even selling some work.

High school led to *UCLA* (*University of California; LA*), the alma mater of both his parents: 'They had a fairly good computer science programme, and it meant that I would be close to my family and friends.' Nachenberg spent six years at *UCLA*, completing a Bachelor's and a Master's degree. One of his 'extracurricular activities' was to act as coordinator for programming contests. He also represented *UCLA* in contests, which he remembers as fun, and a good challenge.

Catching the Bug

While he was at *UCLA*, Nachenberg became involved with *Symantec*, working first on *Norton Commander*, then on *Desktop* for DOS. The next year he worked under Jimmy Kuo – in those days, fifteen people were working on *NAV 2.1*, all on viruses; analysing, writing detection, going on to the next one. Jerusalem was the first virus Nachenberg disassembled – he thinks: 'I remember my first day – Jimmy told me to look at some viruses and see if I could optimize existing signatures to make them smaller. That's how I learned.'

From there, Nachenberg worked with both Kuo and Joe Wells to develop the *NAV 3.0* engine, which is now the foundation for the entire *NAV* product line.

An Integral Position

After this introduction to viruses, Nachenberg worked on checksumming and integrity checking. Then, his opinion of the technique was high; now, however, it is different: 'With viruses like One_Half, we have to ensure that the technology doesn't do more damage than good. Applying technology without forethought could be devastating for the customer.' With the steady increase in virus numbers, however, this man sees developers faced with the inevitability of using a combination of heuristics, known virus detection and integrity checking to keep ahead of everything thrown at them.

Disinfection is another area he believes will change. Though he feels disinfection of program files should only be a last resort, his approach to macro viruses differs markedly: 'With macro viruses,' he explained, 'you have data you cannot always replace; also, because of the nature of macro viruses, a more surgically clean method to remove them is possible. In the end, it's safer, and more important, to repair the data. I strongly advocate repair, with backups, obviously, for *Excel* and *Word* – anywhere there's data involved.'

The advent of the on-access scanner has helped with the virus problem, he says: 'Without real-time scanners, macro viruses would spread largely unchecked and constitute an even larger threat than they do now. Luckily, almost every product has an on-access component, so a good portion of these viruses are caught before they become epidemics.'

What *does* worry him is the rapid increase in macro viruses, and the proliferation of use of the Internet. 'A macro virus can spread as fast as any update,' he explained. 'We're looking into solutions for detecting these threats generically. We're also developing products that stop them before they get to the computer. We look at the content as it goes over the wire, as opposed to waiting till it hits users' hard drives.'

He is also concerned about the possibility of malicious Java applets: 'Right now those applets are saved to disk, and an on-access scanner can detect them just fine. Unfortunately, there is technology where the applet never goes to the disk. They can be sent over the wire directly into a virtual machine; they would never be scanned. The only way you'd be able to catch these things would be as they were coming in over the wire.'

An Industry Forecast

The virus problem, in Nachenberg's opinion, is at the moment manageable, because developers and researchers are beginning to cooperate, and make their findings available to colleagues in other areas of the industry – he cites Joe Wells' WildList to illustrate the point. Additionally, the growth in automation systems is a boon: 'We have,' elaborated Nachenberg, 'constructed a system called SARA that replicates viruses in a virtual machine, analyses them, even writes and tests the definitions – it helps us keep up.'

Nonetheless, he warns against complacency: 'We have to be vigilant. Concept is a prime example: nobody was able to detect it with on-access or on-demand scanners for quite a while, so it spread very rapidly.'

Nachenberg feels that boot sector viruses will decrease in number, due to problems spreading under *Windows 95* and *NT*. ‘It’s macro viruses we have to be concerned about,’ he stated, ‘and problems like ActiveX, Java, and ShockWave – all the Internet agents with executable content.’

Do Unto Others…

Nachenberg is clear in his opposition to virus writing: he has never written self-replicating code, nor does he see it as necessary. It is more useful, in his eyes, to spend fifty hours analysing fifty polymorphic viruses than to spend that time writing one: ‘You get a bigger picture when you analyse many different viruses, as opposed to what you can come up with yourself. I don’t think virus writing needs to be done at all.’

As to what to do about (or to) virus writers, he has conflicting opinions: although he feels action should be taken against people who set out to destroy data; he thinks many virus writers do not have destructive motivation: ‘There’s also an ethical problem,’ he stated. ‘People don’t understand the implications. We have to teach moral issues; ethics should be discussed with reference to the technology.’

Professional Directions

Nachenberg’s position within *Symantec* has developed from part-time programmer to ‘Chief Architect’ of the anti-virus research centre. His relationship with the company consolidated with its sponsoring his Master’s – as his thesis was on polymorphic viruses, the deal was advantageous to both.

With the development of *NAV 3.0*, his involvement with specific analysis has lessened. His role now is twofold: first, engine research and development supporting the research centre; second, researching new technologies. The latter includes looking into Internet threats, automation, heuristics, and emulation technologies: ‘It’s more architectural infrastructure work,’ said Nachenberg, ‘looking forward as opposed to analysing viruses: that was enjoyable for a long time, but it does start to get boring after a while.’

Despite the exodus of *Symantec* employees to competitors in the past couple of years, Nachenberg says he is content, with no desire to leave. He puts that down to changes within the company: ‘There has been a major positive shift in ethic. There’s been a dramatic improvement in the product, and in internal commitment towards technology and the customer.’

Looking Ahead

For now, Nachenberg plans to continue working with virus-related products – he readily admits, however, that his future will almost certainly alter tack: ‘There are more interesting things,’ he confessed, ‘like writing video games! If I get rich, and can do something just for fun, that’s what it would be.’

Returning to the real world, he admits to a passion for cryptography and Internet communications, and also for communicating with people. Gregarious and extrovert, this man is a natural communicator, who enjoys the interaction and stimulus provided by the public side of his work – lecturing and presenting papers for the company.

Carey Nachenberg – the man from *Symantec*.

His interest in this area was instigated in his early university years, when he taught programming classes at a local college: ‘I remember the first class I taught,’ he recalled. ‘In the first lesson, I had to teach people to open and close files. Then I went on to teach classes in assembly and C at *UCLA*. There are many things that people would be interested in if they understood them; the secret is to talk at their level.’

On a Personal Note

Nachenberg is not a fourteen-to-sixteen-hour-a-day programmer: ‘I work a forty-hour week,’ he stated. ‘That’s another thing that’s changing in *Symantec*. There used to be an ethic in our group which said we had to work those twelve-hour days. I find if I work beyond a certain amount of time, I become unproductive. So, I do the best I can; I really give it my all when I’m working, and it’s turned out pretty well. Also, it means I enjoy going to work every day.’

Outside work, Nachenberg enjoys spending his weekends rock-climbing. A recent passion, friends from both *Symantec* and *UCLA* join him regularly – his ambition is to have a long holiday to develop these skills.

He has also bought a house, and said, ‘There seems to be something always broken! But now I don’t live in an apartment any more, I find it interesting; I’m always fixing something, and that occupies a lot of my spare time as well.’

Onward and Upward

Nachenberg’s plans for his professional future already seem well-laid-out: to continue to research new technology, and to learn about the business side of the company, looking at how to make *Symantec* products answer a user’s every wish.

‘Obviously,’ he explained, ‘we should do everything we can to detect the viruses, but many users have different desires from software. Now I’m prioritizing more, and understanding what’s useful to the customers. It’s a new perspective.

‘In twenty years? I couldn’t say what I’ll be doing – hopefully something stimulating; I like the challenge. Anti-virus work is like cops and robbers, always trying to get one up on the bad guy. That’s exciting, and it makes every day fresh. Every day is a new and interesting challenge.’

VIRUS ANALYSIS 1

Packing a Punch

Eugene Kaspersky

Punch is a special virus; not due to its reliability or prevalence in the real world, but because it is another in the long line of virus 'firsts': the first-known memory-resident virus written for *Windows 95*. That is, it infects the Win32 PE (Portable Executable) file format. This virus seems to be paving the way for a new line of *Windows 95* parasitic infectors.

Inside the Code

When a file infected with Punch is executed, the virus drops a VxD (Virtual Device Driver) file to the disk: this dropper contains the virus code, and Punch registers the new driver by including it in the file SYSTEM.INI. The virus then returns control to the host file, and does not otherwise affect the system until the next reboot.

When *Windows 95* next loads, it reads any VxD files from disk, and installs them into memory. Hence, Punch's VxD receives control, hooks some system file access calls, and from there proceeds to infect any *Windows 95* EXE files that are opened. At least, that's the theory.

Fortunately, the virus has several fatal bugs and cannot replicate itself in a standard environment without corrupting *Windows 95* system files to such an extent that the operating system will no longer boot. Thus, the virus has no chance of gaining a foothold in the real world, and will not spread even if it gets into the wild. Unfortunately, however, it would be easy to fix these bugs; thus, a subsequent version of Punch could bring more problems for *Windows 95* users.

The virus contains the text-strings KERNEL32, CreateFileA, WriteFile, ReadFile, SetFilePointer, and CloseHandle. These are used while accessing system resources and functions.

Punch also contains strings which it uses while searching for the *Windows 95* directory. 'QuantumG', the next text-string, is the name of the section the virus inserts into PE files when it infects them. This infector takes its name from the last string which appears in its code: 'Beating You to the Punch in the '97 (almost)'.

Running the Infected EXE File

When an infected file is executed, the virus takes control, and drops the VxD file. To do that, the virus performs the system calls GetLogicalDriveStringsA (KERNEL32 function #350) and SetEnvironmentVariableA (KERNEL32 function #372), and obtains information about system parameters and pointers to the file access system routines CreateFileA, WriteFile, ReadFile, SetFilePointer, and CloseHandle.

Punch then attempts to create the file VVFS.VXD in C:\WIN95\SYSTEM. If that fails (i.e. no such directory), it tries to create the file in C:\WINDOWS\SYSTEM. If that also fails (again, if the directory does not exist), the virus returns control to the host program. Otherwise, it writes 9262 bytes of data and code to the newly-created VxD file.

To complete infection, the virus looks for either the file C:\WIN95\SYSTEM.INI or C:\WINDOWS\SYSTEM.INI, scanning whichever it finds for the string 'ice=' ('device='). If found, Punch inserts the string 'vvfs.vxd,' there. Thus, a string reading 'device=some.vxd' would, after infection, read 'device=vvfs.vxd,some.vxd'.

Before modifying the line, Punch checks to see whether the targeted file contains the string 'vvfs' – if so, the line is not altered. This prevents it multiply adding itself to SYSTEM.INI. Punch then closes the file and control returns to the host.

The result of infection is that there is a newly-created VxD file in the *Windows 95* SYSTEM subdirectory, and the file SYSTEM.INI is modified so that *Windows 95*, while loading, will load and execute this VxD.

Loading *Windows 95* and the IFS API Hook

When its VxD file takes control, the virus checks the version number of the DOS IFS (Installable File System) Manager, hooks some IFS API calls and remains in memory as a VxD.

The IFS API hook operates in a manner similar to that of TSRs under DOS. There are, however, some differences: the hook interposes itself between the IFS Manager and the file system drivers, taking control before the latter are called, and can do whatever it wants.

The virus hook handler intercepts only one function, OpenFile (IFSFN_OPEN), and infects files as they are opened. Punch hooks control when *any* application opens a file, be it a native *Windows 95* application or one for DOS.

Infecting EXE Files

When Punch intercepts a file open call, it reads the file header and checks it for the characters 'MZ' (EXE file marker) and 'PE' (Portable Executable). It then reads other fields from the PE header, creates a new section called 'QuantumG', writes itself to the end of the file (into the newly-created section), and then fixes up the PE header.

Punch also patches the Resources section and the Resources Directory to allow it to access KERNEL32 functions while dropping the VxD file. To prevent duplicate infection, the virus compares the name of the last section in the PE header with the string 'QuantumG' before modifying the file: it does not infect EXE files twice.

Infecting: Final Notes

While infecting, Punch does not access a file's time- and date-stamp; hence the time and date of infected files is modified. Further, the virus does not check a file's attributes: as a result, it will fail to infect Read-only files. Finally, Punch does not check the file's extension, infecting not only *.EXE files, but also DLL, CPL, DRV and other files of PE format.

According to the infection route being followed, the virus writes a different number of bytes to disk: 10185 bytes to the end of an EXE file; 9262 bytes to the VxD file. This is caused by differences between the PE and the VxD file formats – for example, the virus has to have different entry points in the different files. Punch resolves this problem by writing additional code to the EXE file. That code contains the routine which drops the VxD file, and is placed before the main virus code (see Figure 1).

The virus may change the size of EXE files by different values: before writing the new section, it has to increase the file size up to a section alignment. It then writes its 10185 bytes to the end of the file.

Trial

This virus was tested under *Windows 95* (version 4.00.950). The infected file and next generation of the virus dropped the VxD file and modified SYSTEM.INI with no problems or side effects. The headaches began while loading *Windows 95* with the VxD dropper installed. The loading process was not completed – this blue-screened error message appeared:

```
A fatal exception 0E has occurred at xxx:xxxxxx.
The current application will be terminated.
```

Then the system continued booting and another message, 'A fatal exception 0C…', appeared and the system locked up.

After rebooting to DOS, I discovered that the virus had infected the file USER32.DLL in the SYSTEM subdirectory. I replaced the infected file with its original, set the file to Read-only, and again re-booted the computer. This time, the *Windows 95* loading process completed, but was interrupted several times by the system message:

```
This program has performed an illegal
operation and will be shut down. If the
problem persists, contact the program vendor.
```

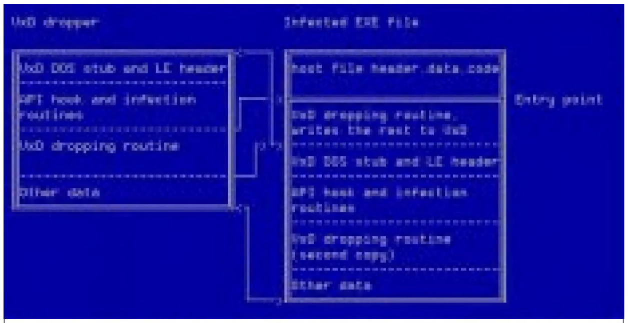

VxD dropper
Infected EXE file
VxD DOS stub and LE header
API hook and infection routines
VxD dropping routine
Other data
host file header.data.code
Entry point
VxD dropping routine, writes the rest to VxD
VxD DOS stub and LE header
API hook and infection routines
VxD dropping routine (second copy)
Other data

Figure 1: Punch exists in two forms; the VxD file version (found in VVFS.VXD) and the EXE file version.

I rebooted to DOS, and searched for and found other infected files: EXPLORER.EXE in the *Windows 95* directory, and in the SYSTEM subdirectory, MPR.DLL, COMCTL32.DLL, MPREXE.EXE, MPRSERV.DLL, MSPWL32.DLL, and SHELL32.DLL.

I restored the infected files and marked all EXE and DLL files Read-Only. *Windows 95* loading was again interrupted by the illegal operation message, and the virus infected the files DESK.CPL and WINSPOOL.DRV (both of which are in PE format). If executable system files in the *Windows 95* directory are marked Read-Only, *Windows 95* loads without problems.

It proved easy to infect several applications, such as WRITE.EXE – in some cases, however, these applications generated an 'illegal operation' message on loading, but would then work correctly. Other problems appeared when I infected goat files, which increased in size by up to 9MB (!).

Conclusion

I have not tested this virus under other releases of *Windows 95*. It is possible that Punch functions 'correctly' only under specific *Windows 95* releases; however, several bugs in the virus which are not release-specific are too lethal to allow the virus to spread outside anti-virus research laboratories.

Even if an infected file were launched on the Internet (as was the case with Hare), Punch would reveal itself in a very short space of time, because of these serious bugs. What must be remembered is that this is only the first TSR virus for *Windows 95*; it is probably not going to be the last.

Punch

Aliases: Punch.9262.

Type: Parasitic Windows 95 PE file infector; uses VxD to stay resident.

Self-recognition in Files:

Text-string 'QuantumG' in last section of PE header.

Self-recognition in Memory:

Cannot infect system memory twice; stays in memory by loading dropper, and writes only one dropper to disk.

Hex Pattern:

```
E800 0000 005D 81ED 0500 0000
8B9D C602 0000 019D CA02 0000
```

Intercepts: ISF API hook OpenFile (IFSFN_OPEN).

Trigger: None known; however, bugs in the virus code result in files being so badly corrupted that the OS no longer boots.

Removal: Under clean system conditions, identify and replace infected EXE files. Look for VxD dropper and delete it, then correct the file SYSTEM.INI.

VIRUS ANALYSIS 2

Share and Share Alike

In these days of hoaxes flooding the Internet, of hype and confusion over the so-called ‘email viruses’, just what the computing world did not need has appeared. ShareFun.A is a recently-discovered *Word* macro virus which attempts to feed off the paranoia and even emulate, in some small way, what Good Times and all the rest were supposed to do.

ShareFun appears in many ways to be an ordinary macro virus (a phrase it would have been impossible to imagine using as little as eighteen months ago). However, it does have a couple of interesting features, and one significant new idea and ‘technology demonstration’.

The virus itself, which appears to have been first discovered in the wild in the US, consists of nine macros. Only two of these are really significant – autoOpen and ShareTheFun.

The AutoOpen Macro

As is well known, any macro called AutoOpen (case is not important) is executed when *Word* opens a document. ShareFun’s AutoOpen macro kicks off by turning off *Word’s* ‘prompt to save NORMAL.DOT’ option, and disabling the execution of auto macros.

Next, it calls a subroutine named ‘SaveAll’, which copies the nine macros from the current document into the document to be infected. For each macro, it calls another subroutine, entitled ‘SaveMacros’, which has a novel technique for obtaining the name of the current file – it uses the FileSummaryInfo command (this function is maintained in *Word 7.0* for backwards compatibility purposes, a fact that serves the virus well). Two of the fields in the information obtained by a FileSummaryInfo are the directory in which the current file is stored, and the file’s name.

Using this information, the virus builds a full pathname for the file in question. It then establishes whether it is copying macros to or from the Global Template (NORMAL.DOT): when the machine is first infected, it will be copying *to* the Global Template, otherwise it will be copying *from* it into a victim document.

After SaveAll has copied the macros, it changes the file type to template. Its method for doing this is interesting: if the name of the file from which the macros are being copied is NORMAL.DOT, it changes the type. If not, it leaves it alone. This is because in the latter case the destination file will be NORMAL.DOT, which is already a template.

Finally, the AutoOpen macro picks a random number (using *Word’s* Rnd function) between 1 and 4. If this number is 3 (a 25% chance), the virus calls the trigger routine.

Passing the *Word*...

The trigger is contained in the macro from which the virus takes its name: ShareTheFun. It uses a WordBasic function called SendKeys, which has been rarely used before in viruses. This function offers the virus author yet more powerful functionality – not only does it (as its name suggests) allow him to transmit keystrokes to *Word*, but it can also give him the opportunity to send the keystrokes to other applications running on the machine.

To the application which receives the keypresses, it will appear that they come from the keyboard – this fact makes the function a simple and fairly powerful tool to control other applications.

ShareTheFun’s first action is to save a copy of the current document (which is infected with the virus) into a file called DOC1.DOC in the root directory of the C drive. It then checks to see if *Microsoft Mail* is running: if so, it makes it the active application (using AppActivate).

If *MS Mail* is not running, the virus kills *Windows* (on *Windows 3.1*, this drops the machine to the DOS prompt; under *Windows 95* it sends it back to the login prompt). This is somewhat noticeable, to say the least.

> *“ShareFun proves that certain things are possible for simple WordBasic viruses”*

Once *Microsoft Mail* is active, ShareFun starts to control it, sending combinations of keys that make up shortcuts to *MS Mail* menu options. First it sends Alt-M, followed by N (compose new message). Next, it chooses three names from the user’s address book, picking a random letter from A to Y (I suspect this is simply an error on the part of the virus author), then a random number, ‘N’, from 0 to 5. It goes to the letter’s entry in the address book, and selects the Nth entry in that letter.

After three names have been chosen, it inserts the text ‘You have GOT to read this!’ into the subject line, and attaches C:\DOC1.DOC (the document saved earlier) to the message. It sends the message, then closes *Mail*.

The Other Macros

ShareFun’s remaining macros are FileTemplates, ToolsMacro, FileClose, FileSave, FileExit, AutoExec, and FileOpen. The first two simply infect the current document (by calling the SaveAll subroutine in the autoOpen macro). The FileClose, FileSave and FileExit macros both first infect the current document and then save it.

The FileOpen macro also infects the current document, but then produces the standard Open File dialog. It needs to do this, otherwise the user is sure to notice that something is amiss as he will be unable to open any documents.

The final macro, AutoExec, is a bit of a puzzler. It consists only of these comments:

```
REM d i n g o a c k
REM DisableAutoMacros
```

DisableAutoMacros is a WordBasic function which does exactly what its name suggests, but the meaning behind the first comment eludes me…

Conclusions

It is important to remember that ShareFun will spread in the normal way for macro viruses – it does not *only* spread via *MS Mail*. However, it is likely that users who do not use *MS Mail* will become suspicious that something is amiss with their system, as *Windows* will shut down 25% of the time they open a document.

As with many other viruses (e.g. Punch – see this issue, p.8), ShareFun is notable not because it is destined to go forth and multiply all that readily in the real world; indeed, it seems unlikely it will do this. Rather, it is a technology-demonstration issue. ShareFun proves that certain things are possible for simple WordBasic viruses – who's to say what will come next?

Presumably support will be built in for a few more *Windows*-based corporate mail systems, coupled with a tidying-up of the virus' behaviour in the absence of such a mailer. Let's hope not, or this new technique could become a real problem, and, dare we say it, bring Good Times one step closer.

ShareFun

Aliases: None known.

Type: MS Word macro infector.

Hex Pattern in Files:

```
84E2 8A8E 8889 E28F 8E82 E28D
8E90 E785 DDEB EFFC EBDA EBEB
```

Trigger: On opening a document in Word, there is a 25% chance that the virus will use a running copy of Microsoft Mail to send an infected document (as an attachment) to three people chosen at random from the address book. The subject line of messages sent in this way is 'You have GOT to read this!' If Microsoft Mail is not running at the time, Windows exits.

Removal: See text.

COMPARATIVE REVIEW

Controlling Your Domain

This month, *VB* takes a slightly different look at the world of the anti-virus product. Stepping into a new area for us, we examine the abilities of anti-virus producers to provide systems to monitor, update, and control their software on remote systems – so-called 'centralised administration'.

Why?

In the modern world, this type of functionality is becoming more important; as corporate networks become both more widespread and more complicated, performing such once-simple tasks as installing upgrades, reconfiguring on-access scanners, and arranging for centralised reporting is becoming unmanageable. One thing anti-virus companies can do to help offset this ever-increasing complexity is to produce software to automate tasks, or to make it possible to apply a single uniform configuration across a selected range of machines.

It is this type of software we are reviewing here. By their very nature, such products are a departure for developers: experienced as they are when it comes to handling viruses, here, such pursuits are secondary to those of distributing data to remote machines, managing multiple configurations, and making the whole complex mess understandable to the user.

Criteria

Most of the products under test are for a *Windows NT* system; however, the range of operating systems over which they will allow control varies fairly widely. Also widely spread are the features incorporated in each product – they range from very basic (*On Technology* and *IBM*), to extremely powerful (*Cheyenne* and *Dr Solomon's*).

Usability is extremely important in such products. The interface should belie the underlying complexities of the problem at hand; for basic tasks, the administrator should not have to resort to the manual. However, with the power some products offer, it is inevitable that certain tasks will necessitate a quick look at the book; it is in cases like this that good on-line help can be… well, a real help.

Other than these fundamental issues, we aim simply to provide an overview of the features available in the marketplace. There are certainly things which had never occurred to the reviewer before as possible, the benefits of which are clear. Equally, however, things which seem easy are not implemented by most or all of the products tested.

It is a reflection of the relative youth of the marketplace for these products that only nine products are included. This does not show undue selectivity on *Virus Bulletin's* part, merely that relatively few products are available, this despite the fact that some companies (for example, *Cheyenne* and *Intel*) have been producing this type of software for a long time now.

There are no scores awarded, and products are not graded in this test. Its purpose is to give an overview of what is still in many ways a fledgling market.

Cheyenne InocuLAN v4

InocuLAN v4 is the latest in the company's long line of accomplished network anti-virus administration utilities. Like its predecessors, it allows comprehensive configuration of servers. Unlike them, however, it allows administration of servers running both *NT* and *NetWare*: a feature those managing heterogeneous networks will greatly appreciate.

The program presents itself well, with a fully-featured *NT* interface. If anything, it is too fully-featured, and can sometimes be tricky to use. It is not always immediately obvious what to do to accomplish certain tasks, and the on-line help does not always present the expected answers. Nonetheless, once the administrator has learnt to navigate the inner depths of the interface, the product does its job exceptionally well.

Machines are grouped together into anti-virus 'domains', and options can be applied to whole domains as easily as to individual machines. Updating is also handled by the utility: it can be configured to download signatures automatically from *Cheyenne's* FTP site or BBS (assuming either an Internet connection or a modem), and distribute them to all machines across the domain.

Unfortunately, the reviewer was able to generate several 'Dr Watson' errors with the product, running on *Windows NT Server 4.0* – it is the nature of such products that it is difficult to say exactly why these happened.

Overall, the system is far more powerful than most of the competitors, but suffers from this in terms of usability. For the high-end user, however, it is a compelling solution.

Dr Solomon's AVTK Server Edition

Beta Three was provided for review: despite the fact that the product was still in beta testing at the time of the tests, it was decided to include it. The decision was well made: the product is both fully-featured and powerful. It offers the ability to group network machines into a series of virtual 'anti-virus domains', each of which can inherit the master configuration settings, or have settings of its own. Indeed, configuration options can be applied at every level (for all domains, each domain, or per machine). New versions of anti-virus client software are placed in the 'Software Repository' – from here they can be used to upgrade client PCs automatically.

The product's ability to start anti-virus software on the client remotely is particularly impressive – if the administrator selects a PC and chooses to install the *AVTK* onto it, the appropriate version is beamed onto the target PC there and then. Clients running *Windows NT*, *95*, and *Workgroups 3.11* are supported in this way. The administrator can request a scheduled scan, not just of the server – the administration utility commands all clients to scan themselves.

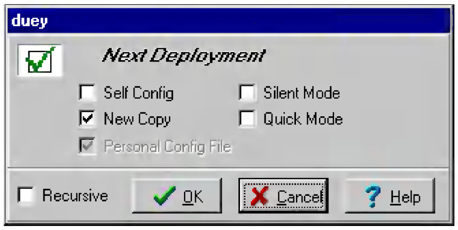
Alerting features also abound: event logs are maintained on the administration machine, and different events can be configured to have different priorities and be routed to different people via a variety of communications media.

The *AVTK Server Edition* brings the product firmly up to date, dragging it kicking and screaming into the *NT*-based 1990s. It offers a powerful feature set. My only major gripe is with the interface: GUIs are meant to make things easy, but the *Server Edition's*, whilst well-implemented, is poorly designed. The drag-and-drop features are at times peculiar, and the context-sensitive menu support strange (menus with one option? Shouldn't double-clicking on the object in question execute that option?). It seems a pity to gripe about this; however, it does detract from the product as a whole. Nonetheless, underneath that interface is a powerful product.

EliaShim Multi-LAN v7.3

Multi-LAN is a new product from Israel-based *EliaShim*, and an interesting one at that. It was tested with *Windows NT* servers, which it detected at install time – the product is able to detect the network type (*NT*, *NetWare*, or 'Other Network') and installs the appropriate software. The *NT* version must be installed from the server console.

The administration interface is called EConsole, and works in a different way from programs provided by other companies for the same purpose. All the others approach the



duey

Next Deployment

☐ Self Config ☐ Silent Mode
☑ New Copy ☐ Quick Mode
☑ Personal Config File

☐ Recursive

problem by assigning software installations to a given *computer* – *EliaShim* assigns them on a per-*user* basis. Given the fact that in most organisations, users always use the same computer and always use it in the same operating system, this seems an odd decision.

EConsole provides a graphical method of configuring which users have access to which products – a user can select various combinations of the three (16-bit, *Windows 95*, and *Windows NT*) *EliaShim* anti-virus products and assign them to users or groups of users.

The theory seems to be (the documentation is not clear on this point) that an update program will run either from the network login scripts or from the startup group on the workstations. However, I could find no documentation or help on this point (indeed, the on-line help file was nowhere to be seen), and the modifications were not performed automatically.

When I modified the user profiles so that login scripts were run, and created login scripts that ran the update program (MAGENT.EXE), the appropriate installation was carried out on logon. This process could certainly be carried out automatically, but until it is, more documentation on the subject is required.

Aside from this glitch, the product worked well. The interface is sufficient under most circumstances to guide the user through the appropriate motions. Centralised logging, reporting and updating are supported as well. A nice product, this – with a little polishing (particularly on the documentation front), it could be a strong contender.

ESaSS ThunderBYTE Anti-Virus for Networks v7.06

ESaSS ThunderBYTE for Networks (*TBAVN*) takes a different approach to the problem of centralised administration. It claims network independence, because it relies on the one thing all PC networking systems have in common: the ability for clients to access shared drives on the server. Therefore, all communication is carried out using shared files. The only problem is one of terminology: it is easy to encounter confusion between the network server and the server for *TBAVN*. In the case of a *NetWare* network, these will not be the same machine. On an *Windows NT* or a *Windows 95* network, they could well be.

Remote workstation system information

System

CPU 80386
MSDOS 6.22
Windows 3.11
Mode 386 enhanced
Free resources 72%
Free memory 6005320 bytes

ThunderBYTE

Version 7.07
License ** Unregistered evaluation version. Do not forget to
Directory C:\TBAV

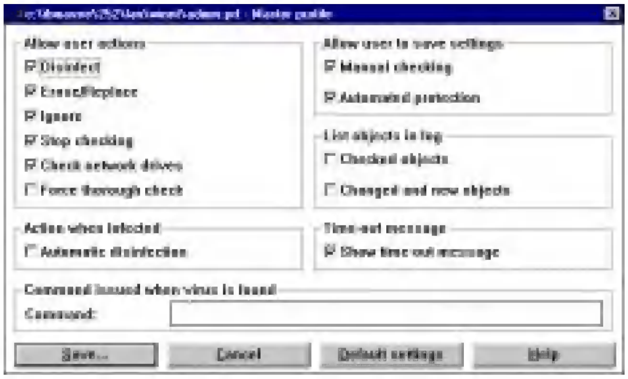
Once installed, the anti-virus administrator's PC is equipped with the *TBAVN* administrator console. Installation copies of client software are placed in a central location on the server; when clients install from there (this could be automated using login scripts), memory-resident software on the client handles commands and scan requests from the server.

The server can request immediate scans of the clients, reconfigure their anti-virus software and examine audit trails of anti-virus events on the network. It even supports a limited scripting language, enabling the administrator to create procedures designed for his particular network.

The major point in *TBAVN's* favour is its network independence. It pays for this in some small way, however, in terms of ease of installation.

IBM AntiVirus v2.5.2

This product allows a fairly limited type of network control: the administrator can create a centralised installation source for the software (by copying the files on the distribution media onto a fileserver), and can also modify the preference files to control what users are and are not allowed to do.



Allow user actions
☑ Disinfect
☑ Erase/Replace
☑ Ignore
☑ Stop checking
☑ Check network drives
☐ Force thorough check

Allow user to save settings
☑ Manual checking
☑ Automated protection

List objects in log
☐ Checked objects
☐ Changed and new objects

Action when infected
☐ Automatic disinfection

Time-out message
☑ Show time out message

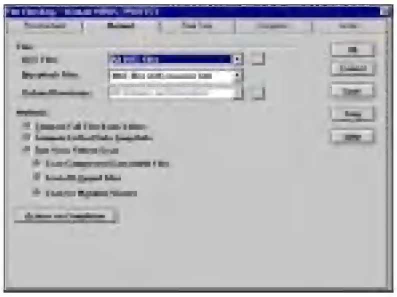
Command issued when virus is found
Command:

Over and above that, there are no facilities for controlling remote PCs, or for changing their configurations. It is possible to arrange for client machines to upgrade their copies of *IBMAV* automatically from the server, however.

Intel LANDesk Virus Protect v4.0

For some time now, *Intel's* product has been well-regarded in the area of centralised administration. This is still true, but they will have to start working along new lines soon if they are to maintain their lead in this area.

LANDesk Virus Protect was tested using *Novell NetWare* servers, as administration facilities are not available on *NT*. Those available under *NetWare* allow the administrator to group his servers into domains, which can then be



configured as one. All aspects of scanning can be configured from the administration program, and cross-server automatic updating can be set up, with signatures being downloaded from *Intel's* FTP site or BBS. The product provides many different methods to notify the administrator in the event of a virus alert.

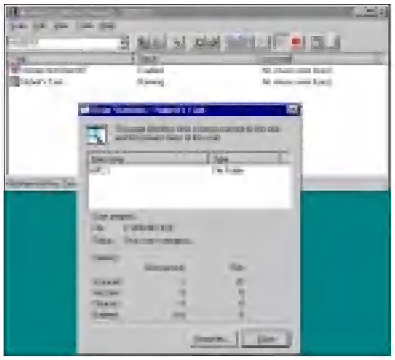
Overall, the product is well-rounded and reliable in this environment; fully-featured and relatively easy to use.

McAfee NetShield for NT v2.5.3

McAfee's NetShield for NT offers limited functionality in the area of remote administration – it is able to connect to other *Windows NT* systems which are running *NetShield* or *VirusScan* and control them as completely as it controls the local machine. Beyond this, however, the product does not offer many labour-saving techniques for the administrator. For the record, *VirusScan* is basically the same program as *NetShield*, the major difference being the lack of ability to connect to remote machines.

With *NetShield*, it is easy to take one job and copy it to another machine using Explorer-like copy and paste. However, if a user decided to give all one hundred machines in your domain the same job, it would have to be done machine by machine.

Automatic updating is supported: both *NetShield* and *VirusScan* support the execution of a command file to retrieve the latest signatures from the *McAfee* FTP site. One way to configure this would be to have one machine download the signatures, and once successfully applied to that machine, to have them copied into a central distribution location (this is also supported) from whence the other machines can retrieve them. Unfortunately, the clients do not automatically detect the fact that there are new signatures available in this central location; they must be told to look there at a certain time, or a certain series of times, using the scheduler.



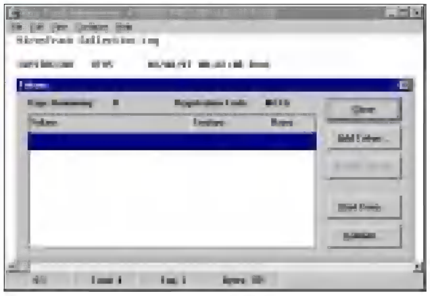
In terms of what it can do, *NetShield* is exceptionally easy to use. However, in the context of this review, it is not at the forefront of technology in terms of features.

On Technology VirusTrack v2.0

On Technology takes a somewhat more low-key approach to the problem of centralised administration – their *VirusTrack* Administrator allows updates to be distributed automatically to workstations on a *NetWare* network. The product also provides a utility to view and filter the network's log files.

Once installed on the *NetWare* server, as users log in, their PCs are inspected, and the version of *VirusTrack* for the appropriate operating system is installed or updated as required. This functionality worked well, but is somewhat basic compared to many of the other products under test.

The administration utility receives alerts (via messages in the log file) from the on-access scanners installed on machines as they log into the network. Subsequent messages from scanners on the clients are logged to the server, and the administration utility can be used to view them. All in all, this product is very basic.

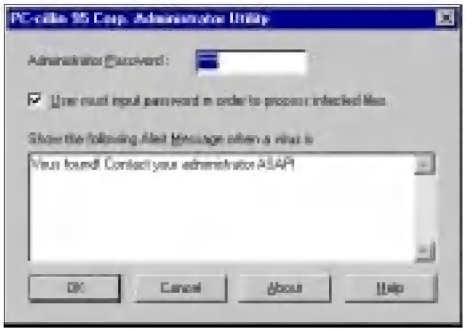


Trend PC-cillin Corporate Version v1.0

The first problem I had when the time came to review this product was figuring out which disk set to use: four hard-to-distinguish sets were contained in the package from *Trend*. Once this barrier was overcome, the product installed without difficulty.

The setup program installed the administration utility on the machine used for installation – this is a simple program which offers three (count 'em!) configuration options: the ability to change the administration password, to select whether or not to allow users to disinfect viruses themselves, and to display a message in times of crisis.

The administrator is given excellent instructions on how to configure his login script system so that workstations will have the software installed at next login, and will be checked on subsequent logins to ensure that the software is up to date. That is about all that the system does, however: no mention is made of centralised logging, or of any other of the possible facilities.


PC-cillin 95 Corp. Administrator Utility
Administrator Password:
☑ User must input password in order to process infected files
Show the following Alert Message when a virus is
OK
Cancel
About
Help

Virus found! Contact your administrator ASAP!

Conclusions

As stated at the start, this review is different from the others which *Virus Bulletin* has carried out in the past. Indeed, only one virus sample was used throughout, and this one simply to test certain alerting features of some products.

Consequently, conclusions are hard to draw. Without the tables of figures and features we have come to expect, it is not easy to rank the products. However, in terms of features, a few products stand apart from the rest.

Cheyenne's InocuLAN and *Dr Solomon's AVTK Server Edition* are particularly noteworthy in this respect – both offer the administrator considerable power. The latter is particularly impressive in its ability to control remote machines running a variety of operating systems.

In other areas, it is worth mentioning *Intel's LANDesk Virus Protect* and *ESaSS' TBAV for Networks* – the latter can be commended for its determination not to depend on any one network or server type.

How to Choose

Any administrator wishing to choose a product to help him in his task of managing the anti-virus software across his network would do well to remember certain things:

- administrators have better things to do than look after anti-virus software
- any company's solution will only help manage that same company's anti-virus products – you cannot simply mix and match one company's products with those of another
- not just the capabilities of the network end of the product line should be considered – there is, after all, no point in administering, maintaining and configuring an anti-virus product which finds no viruses; it is better to spend more time administering a product which does a better job of finding viruses
- take careful account of the different operating systems in use – very few companies use one operating system throughout
- it may well be worth putting up with a powerful product which is harder to use than one which is easy to use but less flexible

Beyond these, however, there is no hard and fast cover-all advice. This market is constantly changing, and it is reasonable to assume that this will continue to be the case for some time to come.

One final thing is clear from the review: as expected, the facilities available from product to product differ a great deal. Some networks, however, may not need the latest and greatest remote-controlled wonder; they may instead simply want something to provide them with basic updating and centralised logging facilities. Sadly, for networks which are larger and more complex, this will probably not be enough.

Products submitted for testing:

Cheyenne InocuLAN
Cheyenne Software Inc
3 Expressway Plaza, Roslyn Heights NY 11577, USA
Tel +1 516 465 5700, fax +1 516 484 1853
http://www.cheyenne.com/

Dr Solomon's AVTK
Dr Solomon's Software Ltd
Alton House, Gatehouse Way, Aylesbury, Buckinghamshire HP19 3XU, England
Tel +44 1296 318700, fax +44 1295 318777
http://www.drsolomon.com/

EliaShim MultiLAN
EliaShim Software
PO Box 25333, Mifrats Haifa (Haifa Bay) 31250, Israel
Tel +972 4 516 111, fax +972 4 852 8613
http://www.eliashim.com/

ESaSS ThunderBYTE AntiVirus for Networks
ESaSS BV
PO Box 1380, NL-6501 BJ Nijmegen, The Netherlands
Tel +31 24 648 8555, fax +31 24 645 0899
http://www.thunderbyte.nl/

IBM AntiVirus
IBM AntiVirus Products
Long Meadow Road, Sterling Forest NY 10979, USA
Tel +1 800 742 2493 (continental US only),
fax +1 914 759 4690
http://www.av.ibm.com/

Intel LANDesk Virus Protect
Intel Corporation
734 East Utah Valley Drive, Suite 300,
American Fork UT 84003-9773, USA
Tel +1 801 328 2000, fax +1 801 756 8349
http://www.intel.com/

McAfee NetShield for NT
McAfee Associates
2710 Walsh Avenue, Santa Clara CA 95051-0963, USA
Tel +1 408 988 3832, fax +1 408 970 9727
http://www.mcafee.com/

On Technology VirusTrack
On Technology (AntiVirus Division)
15 Hamby Road, Marietta GA 30067, USA
Tel +1 770 421 9101, fax +1 770 421 9115
http://www.on.com/

Trend PC-cillin
Touchstone Software Corporation
Huntingdon Beach CA 92648, USA
Tel +1 714 969 7746, fax +1 713 969 1555
http://www.trendmicro.com/

FEATURE

The Indian Subcontinent

Neville Bulsara
N&N Systems and Software

India: a country with the one of the largest populations on the planet. A country whose history dates back over 4000 years; whose fabled riches have lured traders and invaders for æons – Columbus set out to discover it, but failed. A country that won its independence following a creed of non-violence; a country which has produced some of the greatest philosophers of all time.

India: a country whose programmers are among the world's best, and one where viruses abound – as does anti-virus software. This article sets out to document the history of viruses, and their impact on the Indian subcontinent.

How it all Began

Viruses first appeared in India in 1988. Then, I was working as an instructor at a reputed computer training institute: an avid reader of *PC Magazine*, I was astounded at its reports of computer viruses. Despite two years of assembly language programming experience under my belt, I had a tough time figuring out how a program could replicate on its own.

Around July of that year, my workplace was hit by the first virus to appear in India. As I was the only person who could have done anything about it, I was given the responsibility of dealing with it (not that it would have taken much persuasion; I would have foregone a month's salary to be given a shot at it!). The rest, as they say, is history.

Aah, those were the days. Being the first virus I had ever seen, it took me the better part of two days to take it apart. I was hooked: I remember the complicated mechanism Brain employed to lay down its volume label – and of course the trick used to read the original boot sector into what seemed to be ROM (it took me ten whole minutes to figure out that the address wrapped around to point to low memory!).

The Brain virus soon become widespread throughout the country. Considering that many PCs were plain vanilla machines requiring a floppy boot, this was no surprise.

Spreading the Good Word

January 1989 saw India's first seminar on computer viruses, conducted by Captain Rohintan Darukhanawalla and myself under the auspices of the Micro-computer Users' Club (MUC). There were over one hundred attendees, and I had to write a file virus to demonstrate to the participants (I hasten to add that it has never found its way into the wild, nor ever left my machine!). The MUC has since gone to commendable lengths to battle the virus menace.

Around the same time, the Indian government, alarmed by widespread press reports on the 'end of the universe', set up the Department of Electronics Committee on Computer Viruses. The committee was tasked with investigating the impact of the Brain virus on computing as a whole.

I was called on by the committee to assist them: at one time I was asked whether I was sure the virus was not destructive, as another researcher from the subcontinent claimed that it formatted the hard disk after infecting fifty floppies!

Part of the committee's report to parliament stated: 'The Brain virus has not destroyed any data whatsoever and that reports about it having done so are grossly over-exaggerated if not untrue'. What the government did with it, I have no idea. In fact, their silence on viruses as a whole since then makes me wonder if they have classified it under the Official Secrets Act!

1989 – The Game Begins

Things were relatively quiet until July, when I had a call from the secretary of the MUC, who was getting a message on boot-up stating that 'his PC was now Stoned!' (sounds familiar, doesn't it?). He believed the virus had come from one of the shareware disks the club received from others it was in contact with around the world. In the next several days, I had similar calls from people all over the country.

September saw the discovery of the first Indian virus at the Navy's Submarine Base Complex in Bombay. Machines at the base had slowed to a crawl, and I was called in to investigate, and unearthed PrintScreen. A bug meant that its intended trigger routine was never invoked, leading me to remark that version two was probably in the making. Sure enough, it was isolated in December that same year.

This virus was closely modelled on Stoned, which its author had probably studied. Officers at the Submarine Base Complex stated that the virus had come from one of the country's premier educational institutes – this was, however, never substantiated.

November saw the appearance of Joshi – another Indian creation. This virus taught an important lesson: cold boot a suspect system and do not rely on Ctrl-Alt-Del, which the virus can intercept. Jerusalem and Cascade also appeared in 1989: the stage was being set for the creation of an industry which at its peak would play host to over fifty players.

1990: The Golden Year

If there is one thing Indians are good at, it is seeing an opportunity and making the best of it. The unfortunate part is that we try to make the best of it as fast as possible, often to try and make a quick buck. The entry of Dark_Avenger made developers realize that there was money to be made: by January that year there were over fifty anti-virus products on the market. Each of course promised to stop all viruses!

This year also saw the release of a book written by MUC members Suchit Nanda and Harsh Javeri; *War On Virus*: I was its Technical Editor. It was a best-seller, and the three of us went on to conduct seminars throughout the country.

It is with regret that I must note that some local anti-virus software vendors at that time were engaged in developing viruses in order to boost the sales of their products, a stigma which has stuck to players in the game even today. It is not uncommon even now to hear a potential client state that the producers of anti-virus software are those who write viruses.

1990 also saw attempts to train people in 'the art of writing computer viruses'. This led to the development of the 'V3000' (Baobab, now called Quango) virus. At one point, it was even suggested that I was its author!

The year saw the launch of 'the ultimate solution': anti-virus hardware cards. It was alleged that, as such cards took control before anything else, they could stop everything. Some of us warned that they could only monitor DOS after it loaded, but people wouldn't listen. Well… it made lots of money for some!

The rest of 1990 was unremarkable but for the occasional virus. By the last quarter, the influx of new viruses had almost ceased, leading people to believe that the industry was dead or dying. Most of the players had taken their money and run, leaving just a few in the market. Those few would pay for the sins of the others over the years to come.

1991–1995

1991 was unremarkable as far as viruses went. I would not be wrong, however, if I called 1992–1995 the period of the second coming – viruses flooded in. Khobar, Dir-2, Zherkov, One-Half, Die-Hard.4000, Quango, BootExe, Michelangelo Yankee Doodle, Empire.Monkey: you name them, we had them. The most significant, Dir-2, shattered the myth that hardware cards could stop all viruses. Dir-2 grabbed my attention: it took two hours to reverse-engineer it and figure out how it could replicate without hooking interrupts.

1994–1995 saw the first group virus-writing attempt in India. A demonstration virus was sent to me from the 'Pied Pipers'. I have not heard from or of them since, and the virus has never been seen in the wild.

If 1995 were to be remembered for anything, it would be the closure of what was poised to become the country's leading anti-virus company. This vacuum led to what I term the 'second golden age of the anti-virus vendors' in India.

The Great Garage Sale at the End of the Universe

In 1996, a large number of companies produced anti-virus software, some claiming to detect 20,000 viruses (then, there were fewer than 8000 worldwide), some claiming the ability to deal with future 'amœbic' viruses (could someone please explain what that means?), etc. As they say, there's one born every minute and two born to take him…

Notably, it was in this year that Concept, Wazzu, and Rapi – the first macro viruses in India – appeared. Inevitably, the first Indian macro virus, Alien (see *VB*, February 1997, p.10), was also developed. The other important event was the start of The Great Garage Sale at the End of the Universe.

It is always difficult to predict what the future has in store. However, here are a few educated guesses I made last year which perhaps are not far from the truth:

- the days of viruses are numbered – macro viruses are a threat, but will not continue to be so
- many systems in India still use vanilla DOS – this explains why file viruses are more predominant than in countries which are *Windows*-based: this will change
- viruses can be written (and have been) for all platforms: these will not be a major threat, as most viruses are written by people lacking the expertise to write *Windows*-based viruses
- the Internet is the place to watch out for as far as potential entry points for viruses are concerned
- viruses written for *Windows 95* and *NT* (even if posted on the Internet) are unlikely to get far. At worst, only workstations downloading them will be infected. *Windows* viruses do not typically spread within an organization, as people do not share *Windows* applications across workstations.
- *Excel* viruses do not pose a great threat: spreadsheets are of interest only to those within the same organization or in the same industry
- over a period of time (perhaps two to three years in India), the number of new viruses that crop up every month will reduce dramatically. This does not mean that there will be no viruses, but that there will not be enough to support an industry in its own right.
- anti-virus software will be sold as part of a suite of components; an added 'throw-in'. Companies recognizing the inevitable will slash prices long before the collapse, to sell as much as they can while the going is good – the great garage sale at the end of the universe. It has, in my opinion, begun.
- Marketroids will market other products and services. Programmers will find other applications to develop. Researchers will find other fields to research…

And myself? In the future, I hope to preside over the death of the industry I helped, at least in my country, spawn. What could be better than that?

Neville Bulsara is a director at *N&N Systems and Software*. This article represents his personal views and does not necessarily concur with those of the company.

PRODUCT REVIEW 1

diskNET

Dr Keith Jackson

Reflex Magnetics' diskNET provides security and anti-virus features without resorting merely to implementing a virus scanner or similar anti-virus technique. Its approach is more general, similar to *D-FENCE* (reviewed last month), and provides disk encryption and authorization services as well as password protection. Although a *Windows 95* version is available, the version provided (according to a text-string in INSTALL.EXE) was not *Windows 95*-compatible.

Features

diskNET incorporates facilities which restrict diskette access to disks previously authorized by the product. Diskettes modified outside this environment must be reauthorized before they can be re-accessed on a *diskNET*-controlled PC.

diskNET enforces password entry, provides an encrypted drive (formed from a part of the physical hard disk), allows the administrator to scan for viruses, and uses a challenge and response password system. This last is an excellent feature and removes many of the problems associated with having to remember passwords. All in all, a veritable slew of features – the marketing phrases claim it to be a 'Multi-Layered Security Solution'; not relying on scanning alone.

Documentation

The documentation provided comprised a 120-page-long ring-bound A5 manual, incorporating a decent explanation of the error messages and a glossary. The manual warns in strident terms that if you forget the passwords, access to the protected PC will be blocked. You have been warned!

The manual introduces the facilities on offer, and rubbishes relying solely on scanners to prevent a virus attack. The documentation explains clearly why *diskNET* incorporates the concept of an 'administrator' PC, and one or more 'Client' PCs. I found most of the content repetitive, and as a consequence somewhat confusing. Not for beginners, I fear.

My other gripe with it is that some of the explanation of product components is somewhat bereft of technical detail. Descriptions are kept to the bare minimum – not a manual to consult to find out how the product actually *works*. However, it is called a 'User's Guide', so perhaps I'm being a tad harsh.

Installation

diskNET was provided for review on one 1.44MB, 3.5-inch floppy containing 30 files (just under 1MB). As the diskette did not arrive write-protected (this will prove important as I describe how I fared with installation), I write-protected it.

When 'INSTALL' was executed, I was advised to scan all hard drives. After choosing 'Administrator' or 'Client' installation, *diskNET* executed its scanner (*ThunderBYTE* version 7.06, which was current at the time the product was submitted for review).

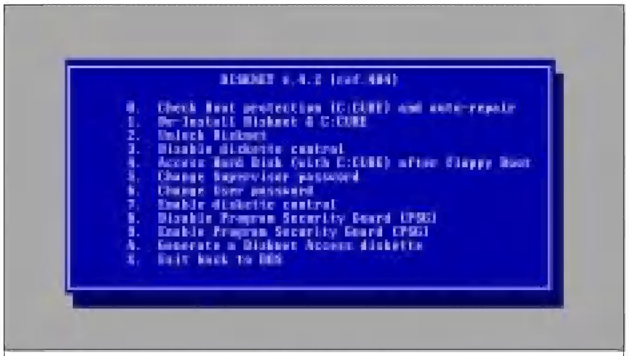
The message did not prevent a scan of my PC. *ESaSS' ThunderBYTE* is known as one of the fastest scanners around – it whizzed through in 45 seconds. In comparison, *Dr. Solomon's AVTK* took 4 minutes 33 seconds; *Sophos' Sweep*, 8 minutes 55 seconds to scan the same disk. *ThunderBYTE* still takes the prize.

Pressing on with installation, I was offered a choice between Express and Custom installation – I chose the former. The installation program then had me select from five installation configurations: diskette authorization only, anti-virus protection, data protection, anti-virus with data protection (which I selected), and maximum protection.

I was then offered another menu where various parts of the product could be included (or not), and the install program then found various other scanners present on my test PC. Each scanner must be confirmed, along with its subdirectory location, and this required many key presses. I even confirmed the location of the *Windows* directory. I would hate to think how many choices must be made for a 'Custom' installation, but it is far better to be sure about such things.

After all this, things ground to a halt when the installation program complained that the diskette used to perform installation was write-protected. The master diskette. I do not understand security products that insist upon writing back to the original master: master disks should be inviolate.

It's not even as if *diskNET* needs this feature because it is copy-protected (which it is not). Although the administrator is not advised to make a copy of the diskette from which to install, *Reflex* states that this is an oversight, and will be corrected in a future version of the documentation.



```
DISKNET v.4.2 (ref.404)

0.  Check Boot protection (C:CURE) and auto-repair
1.  Re-Install Diskset & C:CURE
2.  Unlock Diskset
3.  Disable diskette control
4.  Access Hard Disk (with C:CURE) after Floppy Boot
5.  Change Supervisor password
6.  Change User password
7.  Enable diskette control
8.  Disable Program Security Guard (PSG)
9.  Enable Program Security Guard (PSG)
A.  Generate a Diskset Access diskette
X.  Exit back to DOS
```

diskNET's main screen allows the various components to be executed and controlled.

Administration and Scanning

In express mode, the administrator is responsible for operating the scanner used with *diskNET* – in the other modes (available using the 'custom' setup), users may authorize their own diskettes. The product's anti-virus measures rely chiefly on denying access to unauthorized diskettes, and ensuring that marked files cannot be changed – useful in most situations, but not in others (e.g. development environments where executable files are continually being created). Multiple PCs can be set up by the Administrator in the same mode, using the config files written to the master disk by the install program.

The administrator can elect to use scanners manufactured by other anti-virus developers. The manual suggests using more than one scanner; up to four at a time can be used. It also says that *diskNET* will work with any of 28 scanners on the market; by my calculation, that's most of them – an extremely useful feature, not seen on other such products.

The manual also says: 'Use only the most recent release of the virus scanner. Older scanners may miss new viruses'. Given that the scanner included with this product produced a message warning that it was out of date, this is at best ironic.

Using *diskNET*

When installation was complete, *diskNET* had added nine files to its own subdirectory, seven to the root directory of the hard disk, and one INI file to the *Windows* directory. These files do not take up much space, but I have always objected to programs that clutter up the root directory in this way; they should keep their files in their own subdirectory.

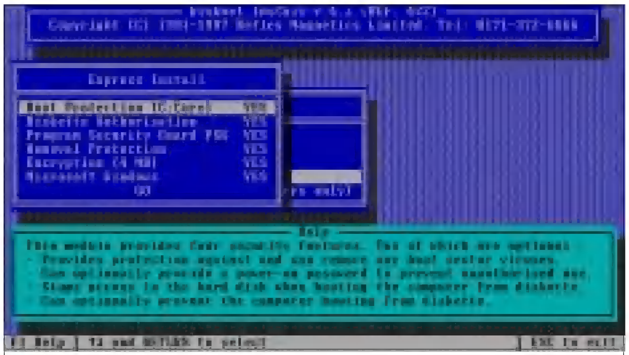
diskNET was fairly frugal with memory usage: DNCRYPT used 4.2KB of RAM, and DNET occupied 8.5KB; a total of 12.7KB. This slightly understates memory usage, as it also takes 1KB of DOS memory before DOS even boots, thus reducing total available memory by a total of 13.7KB.

I did encounter problems when first using *diskNET*; the installation program had tagged a couple of lines to the end of CONFIG.SYS. As my test PC uses a multiple boot system, this meant that the lines (which loaded *diskNET's* device drivers) were never executed. A few minutes' judicious use of a text editor solved the problem, which *Reflex* states does not occur on DOS 6.0 or later.

When booting from a hard disk on which *diskNET* has been installed, a password must be entered before the boot proceeds. Another is then entered to make available any *diskNET*-encrypted hard disk (it is, however, possible to remove the need for this second prompt). If a PC with *diskNET* installed is booted from a diskette, the reboot continues as normal, but the hard disk is then inaccessible.

Encrypted Hard Disk

diskNET offered to make a 4MB encrypted hard disk: the manual explains that this is the minimum allowable size (maximum is 2GB). However, my test PC's hard disk had 21MB available. So what is going on? The manual states that *diskNET* needs a contiguous space for its encrypted hard disk, and suggests defragmenting the disk if the offered size is not as large as desired. I tried this, to no effect. Digging around with *Norton Utilities*, I found two areas flagged as bad blocks: even if these were located at the worst possible place for *diskNET* to obtain a contiguous free space, it should leave room for an encrypted hard disk about 7MB in size. No matter what I did I could not improve on 4MB.



```
[illegible]
Copyright (C) 1991-1997 Reflex Magnetics Limited. Tel: 0171-372-6666

          Express Install
Boot Protection (C:Card)      YES
Diskette Authorization        YES
Program Security Guard PSG    YES
Removal Protection            YES
Encryption (4 MB)             YES
Microsoft Windows             YES
               OK
                                    rs only)

Help
This module provides four security features. Two of which are optional:
 - Provides protection against and can remove any boot sector viruses.
 - Can optionally provide a power-on password to prevent unauthorized use.
 - Stops access to the hard disk when booting the computer from diskette.
 - Can optionally prevent the computer booting from diskette.

F1 Help | ↑↓ and RETURN to select                          | ESC to exit
```

The installation program is simple to use, although it does want to write to the install disk…

An encrypted hard disk is actually a single encrypted file that resides in the root subdirectory of the hard disk. Data stored on the encrypted hard disk cannot be accessed without using *diskNET's* internal encryption/decryption. This technique is similar to that used by compressors such as DriveSpace.

The only details provided in the documentation of the type of encryption used by *diskNET* refer to the key length of the proprietary encryption algorithm. The manual claims that, as a 64-bit key is used, and as the US Government puts severe constraints on software using an encryption algorithm with a key longer than 40 bits, *diskNET's* encryption algorithm must be very strong – a logical non-sequitur if ever there was one.

Program Security Guard

A stand-alone program called PSG can be used to mark selected files (usually executables) to be protected by *diskNET* – PSG is also said to prevent virus tunnelling.

PSG was easy to use, offering a DOS-based windowing system allowing en-masse file selection from a specific subdirectory, or selection of individual files. I am the first to moan about the invasion of *Windows*, but even I admit that PSG's DOS interface looks curiously old-fashioned. Still, it does its job.

Overhead

I tested overhead on program execution of having *diskNET* active by timing how long it took to copy 1.3MB of files from one subdirectory on the hard disk of my test PC to another.

Without *diskNET* active, this test took 22.4 seconds. With *diskNET* active, this copying time remained much the same; actually just over a second faster – but how can something on top of what I used previously make my PC run faster? Whatever the reason, the level of protection offered by *diskNET* (protecting files from deletion or alteration) had no measurable impact on PC operation.

The same cannot be said for using the encrypted hard disk. When the test files were copied to the encrypted disk, copy time rose to 1 minute 23 seconds, an increase of about a factor of four. On more modern PCs, this figure will be much lower – *Reflex Magnetics* quotes figures in the order of 50%. However (as I said in last month's *D-FENCE* review), it would be foolish not to expect a performance hit when using encryption.

diskNET made running the overhead tests rather difficult. To ensure that the same thing is being timed in each test, the files just copied during the test must first be deleted, so the next copy is at the same place on the hard disk. But *diskNET* knew these files were 'protected', and the copies inherited this protection. Thus it would not let me delete the files!

If PC users copy executable files accidentally, they might fill up their hard disk, and not be able to reclaim the space without pestering the administrator. In reality, most users may not even figure out what is happening.

The solution was to use PSG to remove *diskNET* protection from the files, but do remember that it is normally only the Administrator who has access to PSG. The speed at which files can be deleted is not affected by *diskNET*.

Data Authorization

DiskNET incorporates a 'Data Authorization Module' called CHECKDAT. This can be made available on client PCs so that it is not necessary for the Administrator to authorize every single diskette that is used.

CHECKDAT is very easy to use. Too easy – I thought I had authorized the master floppy disk whilst trying to de-install *diskNET*: in fact, I had not. No harm seemed to come to things, but this would not have happened had I not had to leave the disk write-enabled for the installation. Using the write-protect switch to disable writing to all floppies is a habit that should be encouraged: *diskNET* is sending out all the wrong signals.

It is not necessary to use CHECKDAT when a floppy disk is formatted on a *diskNET*-protected PC: these are automatically authorized. This does impose a very small overhead on formatting diskettes. Without *diskNET*, my test PC formatted a 3.5-inch, 1.44MB diskette in 4 minutes 41 seconds, rising to 4 minutes 48 seconds with *diskNET* active.

De-installation

To de-install, first execute the main *diskNET* program and select de-install. This asks if the encrypted hard disk should be removed – the file which forms the encrypted hard disk may be left behind for use at a future date/time.

I needed to use the master disk to de-install, because the install program did not copy the main *diskNET* executable file to the hard disk. Given that this was an administrator's PC, I not sure why it omitted this. All this made de-installation more complicated than it could (and should) have been.

After de-installation, the PATH statements in AUTOEXEC.BAT still pointed to *diskNET*, and a file called DISKNET.INI was left behind in the WINDOWS directory, perhaps because I have no directory called C:\WINDOWS. The only reasonable verdict on this performance: 'Could do better'.

The Rest

diskNET claims to operate with *Windows 3.1*: this is accurate; however, the only *Windows*-specific feature I found was a small program allowing this *diskNET* error message to pop up in a *Windows* box: 'Unauthorized disk in drive A:, scan and authorize disk now?'.

CHECKDOC.DOC, a means of checking for macro viruses, is provided: this file required *MS Word* to be tested. Software entitled 'Tools' is also included, containing the administrator's program, and allows enabling/disabling of *diskNET* options, and edits *diskNET*-specific text messages as desired.

Conclusions

diskNET provides simple-to-use security features that will help prevent viruses gaining access to a PC. It does not impose a noticeable overhead in non-encrypting mode, and has a certain flexibility as an administrator is not necessary.

diskNET should explicitly instruct users to make a copy of the master floppy disk before commencing installation, or should keep any updated files on its own floppy disk. *Reflex* describes this as a feature: by storing the installation configuration on the diskette it is easy to reproduce the same installation on multiple PCs. Readers can make up their own minds on this point.

I had very few problems whilst using *diskNET*, but be aware that using the encrypted hard disk with large amounts of disk access will slow things down, to say the least, noticeably.

Technical Details

Product: *diskNET v4.23* (no serial number visible).

Developer/Vendor: *Reflex Magnetics Ltd*, 31-33 Priory Park Road, London NW6 7UP, UK. Tel +44 171 372 6666, fax +44 171 372 2507, BBS +44 171 372 2584, email sales@reflex-magnetics.co.uk.

Availability: *diskNET* can operate under DOS (v3.3 or above), *Windows* v3.0, v3.1 or v3.11, on any *IBM* XT, AT, PS/2 or 100% compatible PC. A floppy disk (3.5- or 5.25-inch, DD or HD) is required, and 30KB of hard disk space. 70KB more is required if the *Windows*-specific features are installed.

Price: From £24/PC (1000+ PCs) to £125/PC (5-PC licence).

Hardware used: *Toshiba 3100SX*, a 16MHz 386 laptop, with 5MB of RAM, a 3.5-inch (1.44M) floppy disk drive, and a 40MB hard disk, running under *MS-DOS v5.0* and *Windows v3.1.*

PRODUCT REVIEW 2

Dr Solomon's AVTK for NT

Martyn Perry

Dr Solomon's AntiVirus Toolkit for NT (*NTAVTK*) takes centre stage this month. The evaluation set came on seven diskettes: three for the *NT* product, three for DOS, and a 'Magic Bullet' disk. This bootable floppy is intended to provide a clean virus scanner, FindVirus, to run on a FAT-based file system – *Dr Solomon's* and *IBM* are the only companies to provide such a diskette as part of the product. Version 7.68 of the *NTAVTK* scans for 11,037 viruses, Trojans, and variants.

The licence is granted on a per-PC basis, and can be transferred from one machine to another, provided the first can no longer run the programs.

Presentation and Installation

The package comes with documentation for the *Windows NT* scanner, for WinGuard for *NT*, and for the DOS and *Windows* Toolkits. *Dr Solomons'* Virus Encyclopædias are also supplied in addition to the user manuals.

Installation is uncomplicated. Insert the first installation disk and run SETUP.EXE: when prompted, confirm the destination for the program files (C:\WIN32APP\TOOLKIT is the default). Setup copies the files from the three diskettes and adds a new program group to the desktop. After copying is complete, the user chooses whether to run the scheduler at Start-up, and whether to install WinGuard *NT*. These options are presented in reverse order to the documentation.

The WinGuard installation can be deferred. Even if it is, the help file for the program is still loaded, giving the user a chance to look at what the program can do without loading it first. The next installation option asks if the user would like to view the latest README information.

Finally, the disk is scanned, using default settings. This can be terminated and scan settings checked. I would prefer to see the installer given a display of the default options for this initial scan, with the option to defer if necessary.

A full installation adds WinGuard for *Windows NT* and the scheduler to the list of installed services. If WinGuard *NT* is installed, the computer must be restarted for the File System Driver to be loaded; the user can choose to do the reboot immediately after installation, or delay it until later.

Using the Toolkit

The program group includes icons for the Toolkit, its Help file, WinGuard *NT* (if installed), its Help file, the Schedule Editor, its Help file, the Virus Encyclopædia, and an Uninstaller.

A manual scan can be run from the options on the main menu or from the command line. While the scan is running, a progress bar is displayed. The way this bar is calculated appears to be based on the total amount of data on the disk, so if a partial scan of a drive is performed, the bar gives an incorrect indication of the scan's progress.

The scanner can be stopped part-way through a scan and restarted if required. The scan concludes with a summary giving the number and size of files scanned and the amount of time taken.

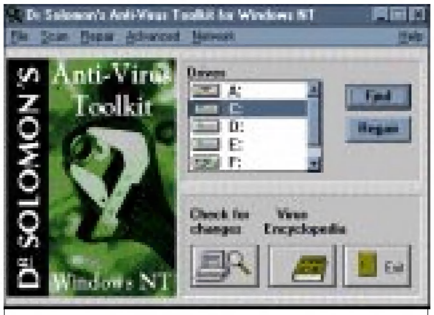
In this version, the default executable file extensions are APP, BAT, BIN, CMD, COM, DEV, DLL, DOC, DOT, EXE, OV?, QLB, SYS, XTP, 001, and 002.

If a virus is detected, the default configuration of *NTAVTK* is to attempt to repair the file concerned. If this is not successful, or cannot be completed for whatever reason, it renames the file so that the first letter of its extension is 'V'; e.g. .EXE becomes .VXE. It is, of course, possible to change this behaviour using the configuration options.

In the past, there has been much debate about the accuracy of disinfections: the preference until recently has been for removal and replacement. The rise of the macro virus, however, means that obtaining a clean copy may not be feasible. Further, loss of the data in the file may be unacceptable to the user. In these circumstances, disinfection is a must. It is also worth remembering that *Word* documents can have any file extension.

A scan may be made of a PC's whole drive or of a specific path and associated subdirectories. The default options provided by the scanner menus will suffice for most requirements – if they do not, *NTAVTK* provides the facility to add, from within the graphical user interface, command-line options to be parsed to the scanner.

While mentioning command-line support, the FindVirus scanner program name under *Windows NT* is WFINDV32. Many of the options available on other platforms are present in this version, including UNC (Universal Naming Convention) support for network drives.



The *NTAVTK* user interface is almost identical to that of *Win3.1* and *Win95*.

The Scheduler

A scheduled scan can be configured to run just once on a certain date and time, or to run periodically, e.g. daily or every two weeks, with an option to disable the event at weekends. Scheduled configuration includes the same scan and action selection as the manual scan.

Scheduled events can be created using the supplied Schedule Editor – the alternative is to edit the event information into a test file. In the latter case, a verification utility can be used to check the syntax of event settings. Event files may have any name, but the active event file is stored under the name TK_SCHED.SDF in the WINNT directory.

The scanner can handle multiple events concurrently. An event can be defined as a scan, a message broadcast, or the execution of another application. The scheduler may be started and stopped via the *NT* Service Control Manager, if required – in normal usage this should not be necessary. In addition, the scheduler keeps a log of its actions in a file called TK_SCHED.LOG.

WinGuard NT

WinGuard *NT* provides on-access (real-time) detection on *NT* machines. Its default configuration is to check executable files when they are executed, copied, opened or renamed. It is possible to configure the resident component to check all files rather than just executables, where executables are defined by the same extension list as in FindVirus, or to exclude boot and partition sectors from the check.

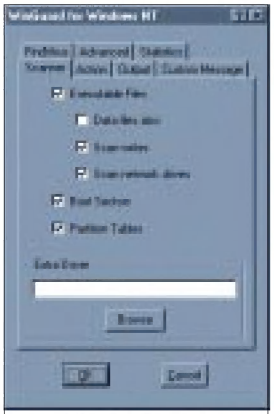
WinGuard *NT* places an icon in the System tray – clicking on this brings up the configuration tabs available. The action options for 'Scan on Reads' are to do nothing or to move the relevant file to the quarantine directory. If 'Scan on Writes' has been selected, the same options are available, with the addition of delete.

Viverify

Viverify, the checksumming component, can be run from within the Toolkit or directly from the command-line. The program has three functions. The first of these is to create a list of files to check – the name of the file in which the list is stored can be user-defined. Files which do change contents legitimately may be excluded in a separate list.

The second function calculates the checksums for the files in the list – a user-defined keyword is used to seed the checksum algorithm. The type of algorithm can be selected depending on the level of security required. Checksumming requires a fair amount of process time, which can be reduced by checking only the first and last 4KB of a file. The program default is to check every fifth byte in the file – this can be adjusted according to whether speed or security is the prime concern.

Finally, Viverify can recalculate the checksums, on demand, and compare with the original list. A list of changed files can be produced in a 'Badlist' file. This file in turn can be used separately by the scanner to check these files specifically for any virus code.



WinGuard for Windows NT

☑ Executable Files

☐ Data files also

☑ Scan macros

☑ Scan network drives

☑ Boot Sectors

☑ Partition Tables

Extra Drives

WinGuard *NT's* configuration screen.

In most environments these days, tools such as Viverify are of minimal use – systems such as *Windows 95* and *Windows NT* have huge numbers of files which will change unpredictably: in such circumstances, the value of checksummers is limited.

Shred

As with other versions of the Toolkit, scan actions do not include file delete. However, the user is provided with a separate facility, called Shred, which can remove a file securely from the system. This can be run either from the main screen's File options menu or from the command-line. In either case, files to be removed can be chosen from a selection box.

When a file is 'shredded', it is overwritten with a series of characters and then deleted – this prevents the file being recovered using an undelete utility, or by viewing the disk with a sector editor.

Virus Encyclopædia

Normally, reviews do not make special mention of associated documentation supplied with the products. However, I feel an exception should be made in this case.

The Virus Encyclopædia, over several years, has provided useful information about various viruses and the impact they have. Having this information both on-line in Help, and in hard copy, provides the best of both worlds: the latest information available on-line with each update, and a facility for the more old-fashioned amongst us who still like browsing real text.

This book, now in its fifth edition, provides information on the more common viruses, a description of the various infection techniques and a brief history of the development of viruses.

Administration

No additional password is required to access the scanner administration. The main menu gives access to the various configuration options, which are:

- File menu: covers deleting a file which cannot be repaired, and loading and saving the configuration file
- Scan menu: deals with running the scanner and checksummer
- Repair menu: tries to repair files or replace corrupted boot sectors on a floppy disk
- Advanced menu: covers access to the scheduler and on-line Virus Encyclopædia

The configuration file, called TOOLKIT.INI, is used to hold a number of settings for the Toolkit programs. Various configurations can be defined for different types of user. The sections in the file cover the scanner and the checksummer.

Reports, Activity Logs, and Updates

A default report is presented on screen when a scan finishes. Further options include one which will send the report to the system printer or a nominated file, and one which will allow *NTAVTK* activities to be reported in the *NT* event log. Scans create entries under the 'FindVirus' category, and scans which find an infection also create an entry under the 'Infection' category.

Updates are provided monthly on write-protected floppies. The file FINDVIRU.DRV contains the virus identification data. An additional driver file, EXTRA.DRV, may be added for newer signatures which occur between updates. Updating involves simply running SETUP from the supplied floppies.

Detection Rates and Real-time Scanning Overhead

The scanner was tested using *VB's* In the Wild, Standard and Polymorphic test-sets. The tests used default scanner file extensions, and the scan action option was selected to move infected files – the residual file count was used to determine the detection rate. This month, results were easy to calculate: no residual files, giving scores of 100% in all three test-sets.

To determine the impact of the scanner on the workstation when it is running, we timed how long it took to copy 200 files (a mixture of EXE and COM) occupying 20.55MB from one directory to another using XCOPY.

The directories used for the source and target were excluded from the scan to avoid the risk of a file being scanned while waiting to be copied. The default setting (Maximum Boost for Foreground Application) was used for consistency throughout. Because of the different processes occurring within the server, the tests were run ten times for each setting and an average was taken. The tests were:

- Program not loaded: establishes the baseline time for copying the files on the server
- Program unloaded: run after the other tests to check how well the server is returned to its former state
- Program loaded without WinGuard running: tests the impact of the application in a quiescent state
- Program loaded with WinGuard loaded but Scan Writes deselected: tests the impact of the real-time scan for just reading the files
- Program loaded, WinGuard loaded, Scan Writes selected: shows the full overhead of real-time scans
- Program loaded with WinGuard loaded with Scan Writes and Immediate scan running: the full impact of running real-time and immediate scanners on files

See the table for the detailed results.

Summary

Installation is quick and easy. The product's interface is identical to the *Windows 3.1* and *95* versions. Scan results are impressive, and underline the consistency of the product's detection rates over a period of years, but it would be nice to see more advantage taken of *NT's* extra functionality.

It is good to see the scheduler as an integral part of the package. Perhaps the only area for criticism is the lack of network or domain support. Having said that, the Toolkit is still getting the fundamentals right.

Dr Solomon's AVTK for NT v7.68

Detection Results

Test-set[1]	Viruses Detected	Score
In the Wild File	476/476	100.0%
In the Wild Boot	86/86	100.0%
Standard	532/532	100.0%
Polymorphic	11000/11000	100.0%

Overhead of On-access Scanning:

The tests show the time (in seconds) taken to copy 200 EXE and COM files (20.55MB). Each test is performed ten times, and an average is taken.

	Time	Overhead
Program not loaded	27.7	–
Program unloaded	28.1	1.5%
Program loaded:		
WinGuard not loaded, no manual scan	28.2	1.7%
WinGuard loaded, no scan writes, no manual scan	53.7	93.7%
WinGuard loaded, scan writes, no manual scan	61.0	120.1%
WinGuard loaded, scan writes, manual scan	110.5	298.7%

Technical Details

Product: *Dr Solomon's Anti Virus Toolkit for NT v7.68*.

Developer/Vendor: *Dr Solomon's Software Ltd*, Alton House, Gatehouse Way, Aylesbury, Bucks, England, HP19 3XU.
Tel +44 1296 318700, fax +44 1296 318777.

Distributor US: *Dr Solomon's Software Inc*, 1 New England Executive Park, Burlington MA 01803, USA.
Tel +1 617 273 7400, fax +1 617 273 7474.

Price: RRP £125+VAT including quarterly updates; £220+VAT including monthly updates.

Hardware Used: *Compaq Prolinea 590* with 16MB RAM and 2GB of hard disk, running *NT 4.0* workstation with Service Pack 1.

[1] Test-sets: For In the Wild file, Standard, and Polymorphic listings, see *Virus Bulletin*, March 1997, p.17. In the Wild boot sector viruses are listed in the January 1997 edition of the magazine; see p.17.

SUBSCRIPTION RATES

Subscription price for 1 year (12 issues) including first-class/airmail delivery:

UK £195, Europe £225, International £245 (US$395)

Editorial enquiries, subscription enquiries, orders and payments:

Virus Bulletin Ltd, The Pentagon, Abingdon Science Park,
Abingdon, Oxfordshire, OX14 3YP, England

Tel 01235 555139, International Tel +44 1235 555139
Fax 01235 531889, International Fax +44 1235 531889
Email: editorial@virusbtn.com
World Wide Web: http://www.virusbtn.com/

US subscriptions only:

June Jordan, *Virus Bulletin*, 590 Danbury Road, Ridgefield,
CT 06877, USA

Tel +1 203 431 8720, fax +1 203 431 8165

No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.

END NOTES AND NEWS

Anti-virus, access control, and security software developer *Global Data Security Inc* has announced its acquisition of the LANExpert division of *Horizons Technology*. *GDS* publishes access control products *Protec* and *Protec Net*, and holds **exclusive North American licences for *Reflex Magnetics diskNET*** (see review on p.18). For information on the company, contact Jim Harris of *GDS (Europe)*; Tel +44 191 916 4354.

InfoSecurity 1997 will take place at Olympia 2 (London, England) from 29 April–1 May 1997. The event is planned to address all aspects of IT security in the business environment, and many anti-virus developers will be present. For information, contact Yvonne Eskenzi on Tel +44 181 449 8292, or on the Web at http://www.infosec.co.uk/.

Software developers *Data Fellows* has announced the release of version 3 of its flagship product, *F-PROT Professional*. Also being launched by the company is *F-Secure VPN*, an encrypting router, and the *F-PROT Professional NT Server.* For information, contact the company on Tel +358 9 478444, or visit the Web site at http://www.datafellows.com/.

A study just released by *IBM* reveals that **nearly one in four computer users claim past infection by computer viruses**. Despite this, the company states that the survey they conducted shows only two-thirds of users having an anti-virus program on their computer. Further information can be obtained from the company; Tel +1 512 434 1554, http://www.av.ibm.com/.

***Sophos Plc's* next round of anti-virus workshops** will be on 21/22 May 1997 at the training suite in Abingdon, UK. The company's training team is also hosting a Practical *NetWare* Security course on 13 May 1997 (cost £325 + VAT). Information is available from Julia Edwards, Tel +44 1235 544028, fax +44 1235 559935, or access the company's World Wide Web page; http://www.sophos.com/. The company has also announced that its *SWEEP for Windows NT* now features automatic distribution of updates to all *NT* workstations and servers. Free evaluation copies of this and other *Sophos* products can be downloaded from the company Web site (see address above).

The **1997 *DECUS* conference will take place from 7–10 April** at the University of Westminster in the UK. The event will cover a wide range of topics, and, in addition to the presentations, delegates will also be able to attend various half- and full-day seminars. For information, contact the *DECUS* registration line; Tel +44 118 920 2182, fax +44 118 920 2211.

Symantec Corporation has announced a new technology to counteract the macro virus threat in corporate environments: according to a recent press release, the **Macro Virus Protection System** will be available to the company's corporate customers by 1 May 1997, and initial support will be for *NAV 2.0 for Windows 95* and for *Windows NT*. Information is available from the *Symantec* Web site; http://www.symantec.com/.

Dr Solomon's Software Ltd (formerly *S&S International*) is presenting **Live Virus Workshops** in the UK on 15/16 April and 13/14 May 1997. Details are available from Melanie Swaffield at *Dr Solomon's*; Tel +44 1296 318700, Web site http://www.drsolomon.com/. The company has also launched a system for automatic virus protection for the home PC. *HomeGuard* is said to protect home PCs against viruses from the Internet, email, CDs, and floppy disks, and will be sold through major retail outlets.

ON Technology Corporation has announced the release of a **new version of its *On Guard Internet Firewall*** which is designed to simplify installation, configuration, and management of an Internet firewall. Further details are available from Maggie Davies, email maggied@cix.compulink.co.uk, or Tel +44 1344 301022.